



ksmbd: fix use-after-free and NULL deref in smb_grant_oplock()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-31444 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-22 14:16:38 UTC |
| Updated | 2026-04-22 14:16:38 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free and NULL deref in smb_grant_oplock()

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|-----------------------|-----------------------|--|
| CNA | Linux | Linux | affected 302fef75512b2c8329a3f5efab1ae7ba2562387a 9e785f004cbc56390479b77375726ea9b0d1a8a6 git |
| CNA | Linux | Linux | affected 08aa9f3c8cf4d0bee44df540dfe34e8d64069f2c 7de55bba69cbf0f9280daaea385daf08bc076121 git |
| CNA | Linux | Linux | affected 1d6abf145615dbfe267ce3b0a271f95e3780e18e a5c6f6d6ceefed2d5210ee420fb75f8362461f46 git |
| CNA | Linux | Linux | affected ce8507ee82c888126d8e7565e27c016308d24cde 6d7e5a918c1d0aad06db0e17677b66fc9a471021 git |
| CNA | Linux | Linux | affected 1dfd062caa165ec9d7ee0823087930f3ab8a6294 48623ec358c1c600fa1e38368746f933e0f1a617 git |
| CNA | Linux | Linux | affected 6.6.130 6.6.131 semver |
| CNA | Linux | Linux | affected 6.12.78 6.12.80 semver |
| CNA | Linux | Linux | affected 6.18.19 6.18.21 semver |
| CNA | Linux | Linux | affected 6.19.9 6.19.11 semver |

References

| Reference | Source | Link | Tags |
|---|--------------------------------------|---|---------|
| git.kernel.org/stable/c/6d7e5a918c1d0aad06db0e17677b66fc9a471021 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/a5c6f6d6ceefed2d5210ee420fb75f8362461f46 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/9e785f004cbc56390479b77375726ea9b0d1a8a6 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/7de55bba69cbf0f9280daaea385daf08bc076121 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/48623ec358c1c600fa1e38368746f933e0f1a617 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)